UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/575,424	04/10/2006	Yang Peng	CN 030035	3752

24737 7590 03/08/2011
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	PAPER NUMBER
2491	

NOTIFICATION DATE	DELIVERY MODE
03/08/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

vera.kublanov@philips.com
debbie.henn@philips.com
marianne.fox@philips.com

Office Action Summary	**Application No.** 10/575,424	**Applicant(s)** PENG ET AL.	
	Examiner JEFFREY D. POPHAM	**Art Unit** 2491	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2010*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-32* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 April 2006* is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Remarks

Claims 17-32 are pending.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/28/2010 has been entered.

Response to Arguments

2. Applicant's arguments filed 11/29/2010 have been fully considered but they are not persuasive.

Applicant argues, once again, that "authentication of any computing device on the network is not the same as authentication of media content downloaded from that device. While the computing device might be authentic, the media content residing on that computing device might be compromised." However, the claims are not directed to authenticating content that is stored on a server, but rather, the claims are directed to authenticating content after the content is downloaded. The claims do not state that the downloadable content is signed prior to storage on any server, therefore, any argument of Applicant's with respect to authenticating content while it is stored on a device other than the client is moot.

Applicant goes on to argue that Kambayashi does not disclose “each external media content having an added private key associated with at least one stored media content.” However, Kambayashi teaches that each piece of external media content sent from the server is encrypted with a private key. This private key is associated with “at least one stored media content” as it is used to encrypt the external media content that is associated with (or is, itself) a piece of stored media content. The claims do not state that the private key cannot be a key held by a server and, as Applicant does not claim how this association occurs, the association provided by Kambayashi reads thereon. Any key that encrypts the content (which corresponds to the claimed “having an added private key” of claim 17, for example) is clearly associated with that content since the content is encrypted therewith.

Applicant goes on to argue that Kambayashi does not teach verifying “the authenticity of the downloaded external media content using the public key read-out from the optical disk and the added private key of the downloaded external media content”, as for example recited in claim 20. While it is admitted at page 9 of the Final Office Action that Kumbayashi does not teach reading the public key from the optical disk, it is respectfully submitted that Kumbayashi does nothing to suggest “added private key of the downloaded external media content"." As previously explained, in a public key encryption system in which a private key has encrypted the data, one simply cannot use both the public key and private key for verifying authenticity, otherwise, one will wind up with encrypted data or gibberish. In a public key encryption system, the private key or public key may be used to encrypt the data. In the claims, the private key is used to encrypt the data. Then the public key, and only the public key, can be used to decrypt the data to verify authenticity thereof. If one uses both the public key and private key to decrypt the data, the data will not be properly decrypted and either encrypted data or gibberish will remain. This use of both the private key and public key does not have basis in the application as originally filed and the limitation is indefinite for failing to point out and distinctly claim the appropriate subject matter. 112 rejections are provided below with additional analysis. It is also noted that claims 24 and 31 were previously objected to for this precise issue, and Applicant amended the claims to overcome the objection. However, Applicant then put the same subject matter into the independent claims.

Applicant goes on to state “Also see the arguments above and in the responses to the previous Office Actions with regard to the authentication of the external content independent of the authenticity of the computing devices, e.g., servers, on which such external content resides.” Applicant is directed to the previous responses, such as the final office action dated 9/28/2010 for a complete response to these previous arguments. As explained in the final office action dated 9/28/2010, Kambayashi explicitly provides for the distinction between authentication of the server and authentication of the content. As an example, figure 21, step S406 teaches determining whether the server is certified (authentic). In step S409, it is determined whether the data is certified (authentic). Clearly, providing separate steps for authenticating the server and authenticating the data shows that authentication of the data is separate from authenticating the server. Step S409 (certification of the ENAV/V-click data) is further discussed with respect to figure 22. Figure 22 clearly shows decoding the data using the public key P_k, decoding the data using content ID (CID), and determining whether the data is certified (authentic). Kambayashi further states that "the certification of the server 7 that provides ENAV contents 103 or that of V-click data, or both may be omitted." As one can see, since authentication of the server can be omitted, this would leave authentication of the content remaining, which is certainly separate from that of the server, since authentication of the server is not performed. It is also noted that Applicant's arguments with respect to servers are moot as the claims are not directed to authenticating any data while the data is stored on the server, providing the data from any server, or any server whatsoever.

Applicant also argues that "Uranaka describes a server public key, e.g., distribution descriptor 23 recorded in the burst cutting area of the DVD, (see, Uranaka, col. 12, lines 12-15) for verifying authenticity of the specific server. As such, it is respectfully submitted that Uranaka does not cure the deficiencies of Kumbayashi and in fact, shares the shortcomings of Kumbayashi in teaching authentication of a server." As described above, Kambayashi clearly and explicitly teaches authentication of the server and authentication of the data as separate steps. While it may be the case that the server's private key is used to encrypt the data, this does not detract from the fact that the private key is associated with the content since the content is encrypted therewith, nor does it detract from the fact that the data is authenticated using a public key associated therewith. Kambayashi already teaches that the client acquires the public key in order to authenticate the data, and Uranaka is only used in the rejection of claim 20 for teaching that the public key is read from the optical disk. This will be the public key of Kambayashi that was just described and is used to authenticate the data.

Applicant finally argues that Kambayashi in view of Uranaka does not teach the entirety of claim 20, without providing any supporting arguments. Due to what Applicant has highlighted in this block copy of claim 20, the above responses to arguments are deemed sufficient.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 17-32 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 20 claims "a control system to verify the authenticity of the downloaded external media content using the public key read-out from the optical disk and the added private key of the downloaded external media content before the stored media content is played in coordination with the associated downloaded external media content". The application as originally filed does not provide basis for using both the public key and private key at a control system in an optical disk player for verifying authenticity of the data. To the contrary, the application as originally filed provides for adding the private key to the content at a separate device (that is, encrypting the content with the private key), downloading the content to the player, and then verifying authenticity at the player using the public key. Each of the other independent claims has the same issue and are rejected for the same reasons. Furthermore, all dependent claims also have the same issue and are rejected for the same reasons.

Furthermore, claim 24 states that "the control system verifies the authenticity of the downloaded external media content by performing asymmetric cryptography using the public key stored on the optical disk corresponding to the added private key encrypted in the downloaded external media content." However, the "added private key" of claim 20 is added to the content by encrypting the content, as this is the only manner in which the adding has basis in the application as originally filed. Nowhere does the application as originally filed state that the private key is encrypted along with the downloaded external media content. For purposes of prior art rejection, this has been construed as "the control system verifies the authenticity of the downloaded external media content by performing asymmetric cryptography using the public key stored on the optical disk corresponding to the added private key used to encrypt the downloaded external media content". Claim 31 has the same issue.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 17-32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 20 claims "a control system to verify the authenticity of the downloaded external media content using the public key read-out from the optical disk and the added private key of the downloaded external media content before the stored media content is played in coordination with the associated downloaded external media content". However, when one looks to the written description, it appears as though this public key and private key are the 2 keys of an asymmetric key pair (Page 7, for example, showing that the private key used to sign the downloaded content and the public key that is stored on the disk are part of the same key pair). One will further note that the control system only has access to the public key retrieved from the optical disk, and never sees the private key at all. Furthermore, if the control system were to use both the private key and public key in verifying authenticity of a piece of data, the operations would cancel each other out, since one key would encrypt and the other would decrypt. Since the downloadable content of the claims is already encrypted with the private key, only the public key can verify authenticity thereof. Use of the private key again would either result in encrypted data (which will never verify authenticity of the data) or gibberish, depending on the encryption algorithm used. For purposes of prior art rejection, the pertinent limitation has been construed as verifying authenticity using only the public key that is associated with the private key.

Claim Objections

5. Claims 24 and 31 are objected to because of the following informalities: As described above, claim 24 does not have basis in the application as originally filed due to reference to "the added private key encrypted in the downloaded external media content." This also does not have proper antecedent basis in claim 20. Claim 31 has the same issue, and the claims have been construed as described above.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 17, 18, 20, 22, 24, 25, 27-29, 31, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kambayashi (U.S. Patent Application Publication 2004/0001697) in view of Uranaka (U.S. Patent 6,470,085)

Regarding Claim 20,

Kambayashi discloses an optical disk player comprising:

An optical disk driver unit to read out stored media content provided on an optical disk on which the stored media content is stored (Figures 1 and 18; and Paragraph 47);

A public key which is used for authenticating external media content having an added private key (Figures 21-22; and Paragraphs 216-221 and 231-244);

A network interface to download one or more external media content, each external media content having the added private key associated with at least one stored media content, the one or more external media content provided on one or more computing devices distributed on a network (Figures 1, 18, and 21-22; and Paragraphs 205, 209, 212, 216, 240, and 246); and

A control system to verify the authenticity of the downloaded external media content using a public key that was obtained and is associated with the added private key of the downloaded external media content before the stored media content is played in coordination with the associated downloaded external media content (Figures 21-22; and Paragraphs 216-221 and 231-244);

Wherein the authenticity of the external media content is verified unaware of the authenticity of the one or more computing devices on which the external media content is provided (Figures 21-22; and Paragraphs 216-221 and 231-244);

But does not appear to explicitly disclose that the public key is read from the optical disk.

Uranaka, however, discloses that the public key is read from the optical disk (Column 6, lines 42-54; Column 7, lines 9-33; Column 8, lines 23-41; and Column 12, lines 12-15). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content usage control system of Uranaka into the enhanced content reproduction system of Kambayashi in order to ensure that a user has been given an appropriate public key by sending it on the disk along with the content, and/or to allow the system to restrict content access to those devices that a server deems authorized to do so.

Regarding Claim 17,

Claim 17 is a system claim that is broader than player claim 20 and is rejected for the same reasons.

Regarding Claim 25,

Claim 25 is a method claim that is broader than player claim 20 and is rejected for the same reasons.

Regarding Claim 22,

Kambayashi as modified by Uranaka discloses the player of claim 20, in addition, Kambayashi discloses that the downloaded external media content is an application program (Paragraph 220, script in ENAV contents, for example).

Regarding Claim 29,

Claim 28 is a method claim that is broader than player claim 29 and is rejected for the same reasons.

Regarding Claim 24,

Kambayashi as modified by Uranaka discloses the player of claim 20, in addition, Kambayashi discloses that the control system verifies the authenticity of the downloaded external media content by performing asymmetric cryptography using the public key stored on the optical disk corresponding to the added private key used to encrypt the downloaded external media content (Figures 2—22; Paragraphs 216-221 and 231-244).

Regarding Claim 31,

Claim 31 is a method claim that is broader than player claim 24 and is rejected for the same reasons.

Regarding Claim 18,

Kambayashi as modified by Uranaka discloses the system of claim 17, in addition, Uranaka discloses that the public key is stored in a BCA zone of the optical disk (Figures 2 and 4; Column 5, lines

20-42; Column 5, line 58 to Column 6, line 5; and Column 8, lines 34-41).

Regarding Claim 27,

Kambayashi as modified by Uranaka discloses the method of claim 25, in addition, Kambayashi discloses that the coordination between the read out stored media content and the downloaded external media content will not be established if the downloaded external media content is not authenticated (Figures 21-22; and Paragraph 234).

Regarding Claim 28,

Kambayashi as modified by Uranaka discloses the method of claim 27, in addition, Kambayashi discloses that the coordination between the read out stored media content and downloaded external media content will be established if the downloaded external media content is authenticated (Figure 21; and Paragraph 234).

Regarding Claim 32,

Kambayashi as modified by Uranaka discloses the method of claim 25, in addition, Kambayashi discloses that the optical disk comprises digital information stored thereon, the stored digital information comprising network address information that is used to download the external media content (Paragraph 209); and Uranaka discloses that the optical disk comprises the public key that is used to verify the authenticity of the downloaded external media content before playing the stored media content in coordination with the external media content (Figures 2 and 4; Column 5, lines 20-42; Column 5, line 58 to Column 6, line 5; and Column 15, lines 57-67).

7. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kambayashi in view of Uranaka, further in view of Ryan (U.S. Patent 5,754,648).

Kambayashi as modified by Uranaka does not explicitly disclose that the public key is stored in a media content zone of the optical disk.

Ryan, however, discloses that the public key is stored in a media content zone of the optical disk (Column 3, lines 47-67; and Column 8, lines 31-37). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the media security and tracking system of Ryan into the enhanced content reproduction system of Kambayashi as modified by Uranaka in order to allow the system to provide additional authentication and authorization steps such that a device can ensure that both the disk and device are authentic and authorized for use with each other by using data stored on the optical disk itself and data stored on a magnetic track attached to the disk, thus decreasing the chance of unauthorized use thereof, and/or to provide the ability to track use of the media.

8. Claims 21 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kambayashi in view of Uranaka, further in view of Collins (U.S. Patent Application Publication 2002/0073316).

Regarding Claim 21,

> Kambayashi as modified by Uranaka does not explicitly disclose that the control system detects whether the downloaded external media content is integral before verification, wherein the verification will not be executed if the downloaded external media content is detected to not be integral.
>
> Collins, however, discloses that the control system detects whether the downloaded external media content is integral before verification, wherein the verification will not be executed if the downloaded external media content is detected to not be integral (Paragraphs 73-77; detecting whether the downloaded content is “integral” may comprise either, or both, verification of the program packet format and/or verification of the checksum, each of which must succeed before signature verification is performed). It would have been obvious to one of ordinary skill in the art at the time of applicant’s invention to incorporate the content authentication and access control system of Collins into the enhanced content reproduction system of Kambayashi as modified by Uranaka in order to allow the system to detect when errors in the data have occurred, such that data with errors will not be allowed to be

processed and only correct data will be processed, and/or to ensure that the data is proper and authentic before allowing access to proceed, thereby increasing security of the system by ensuring both integrity and authenticity of the content.

Regarding Claim 26,

Claim 26 is a method claim that is broader than player claim 21 and is rejected for the same reasons.

9. Claims 23 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kambayashi in view of Uranaka, further in view of Tsumagari (U.S. Patent Application Publication 2004/0126095).

Regarding Claim 23,

Kambayashi as modified by Uranaka does not explicitly disclose that the application program is a JAVA language application program.

Tsumagari, however, discloses that the application program is a JAVA language application program (Figure 10; and Paragraphs 143 and 167). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the script execution system of Tsumagari into the enhanced content reproduction system of Kambayashi as modified by Uranaka in order to allow the system to work with various kinds of well-known languages, thereby allowing additional flexibility in the creation of ENAV contents as well as allowing a broader range of devices to take advantage of the ENAV contents.

Regarding Claim 30,

Claim 30 is a method claim that is broader than player claim 23 and is rejected for the same reasons.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ashok Patel can be reached on (571)272-3972. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Primary Examiner
Art Unit 2491

/Jeffrey D Popham/
Primary Examiner, Art Unit 2491